

Sub B1 network

a processor programmed to authenticate a plurality of users on the computer network for secure processing of a value bearing item, wherein the processor includes a state machine for determining a state corresponding to availability of one or more commands;

an interface for communicating with the computer network.

3. The cryptographic device of claim 1, wherein the state machine includes an initialized state.

4. The cryptographic device of claim 1, wherein the state machine includes an operational state.

5. The cryptographic device of claim 1, wherein the state machine includes an administrative state.

6. The cryptographic device of claim 1, wherein the state machine includes an exporting shares state.

7. The cryptographic device of claim 1, wherein the state machine includes an importing shares state.

1 8. The cryptographic device of claim 1, wherein the state machine includes an error state.

5 9. The cryptographic device of claim 2, wherein the one or more commands corresponding to the uninitialized state includes a command for start initializing.

10 10. The cryptographic device of claim 3, wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands.

15 11. The cryptographic device of claim 4, wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support.

20 12. The cryptographic device of claim 11, wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command.

25 13. The cryptographic device of claim 11, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

30 14. The cryptographic device of claim 11, wherein the commands for key management include one or more of export

1 transport public key command, start importing MKS command, create
MKS shares command, generate MKS command, activate MKS command,
delete dormant MKS command, global decrypt and MAC command,
compute MAC command, verify MAC, and encryption and MAC
5 translation commands.

15. The cryptographic device of claim 11, wherein the
commands for audit support include one or more of create audit
entry command, create audit key command, and export audit
10 verification key command.

16. The cryptographic device of claim 5, wherein the one
or more commands corresponding to the administrative state
include commands for one or more of create account command,
15 delete account command, modify account command, view access
control database command, end admin. command, logon command,
logoff command, query current user role command, query current
user ID command, set clock command, get status command, session
management commands, and audit entry creation command.

17. The cryptographic device of claim 6, wherein the one
or more commands corresponding to the exporting shares state
include commands for one or more of logon command, logoff
command, query Current User Role command, query current user ID
25 command, export share command, abort export command, get status
command, session management commands, and audit entry creation
command.

18. The cryptographic device of claim 7, wherein the one
30 or more commands corresponding to the importing shares state
include commands for one or more of logon command, logoff
command, query current user role command, query current user ID
command, export transport public key command, import share
command, combine shares command, set status command, session
35 management commands, and audit entry creation command.

1 19. The cryptographic device of claim 8, wherein the one
or more commands corresponding to the error state include
commands for one or more of get status command, and access
control queries command.

5 20. The cryptographic device of claim 1 further comprising
computer executable code to keep track of a present operational
state.

10 21. The cryptographic device of claim 1, wherein the
processor is programmed to verify that the authenticated user is
authorized to assume a role and perform a corresponding
operation.

15 22. The cryptographic device of claim 1, wherein the
cryptographic device includes a computer executable code for
preventing unauthorized disclosure of data.

20 23. The cryptographic device of claim 1, wherein the
cryptographic device includes a computer executable code for
supporting multiple concurrent users and maintaining a separation
of roles and operations performed by each user.

25 24. The cryptographic device of claim 1, wherein the value
bearing item is a postage value including a postal indicium.

 25. The cryptographic device of claim 24, wherein the
postal indicium comprises a digital signature.

30 26. The cryptographic device of claim 24, wherein the
postal indicium comprises a postage amount.

35 27. The cryptographic device of claim 24, wherein the
postal indicium comprises an ascending register of used postage
and descending register of available postage.

1 28. The cryptographic device of claim 1, wherein the value
bearing item is a ticket.

5 29. The cryptographic device of claim 1, wherein the value
bearing item includes a bar code.

 30. The cryptographic device of claim 1, wherein the value
bearing item is a coupon.

10 31. The cryptographic device of claim 1, wherein the value
bearing item is currency.

 32. The cryptographic device of claim 1, wherein the value
bearing item is a voucher.

15 33. The cryptographic device of claim 1, wherein the value
bearing item is a traveler's check.

20 34. The cryptographic device of claim 1, wherein each
security device transaction data includes an ascending register
value, a descending register value, a respective cryptographic
device ID, an indicium key certificate serial number, a licensing
ZIP code, a key token for an indicium signing key, user secrets,
a key for encrypting user secrets, data and time of last
25 transaction, last challenge received from a respective client
subsystem, an operational state of the respective device,
expiration dates for keys, and a passphrase repetition list.

30 35. The cryptographic device of claim 1, wherein each
security device transaction data includes information to define
the present operational state of the device.

35 36. The cryptographic device of claim 1, wherein the
processor is capable of sharing a secret with a plurality of
other cryptographic devices.

5 38. The cryptographic device of claim 37, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

40. The cryptographic device of claim 1, wherein the
15 cryptographic engine is programmed to perform one or more of
Rivest, Shamir and Adleman (RSA) public key encryption, DES,
Triple-DES, DSA signature, SHA-1, and Pseudo-random number
generation algorithms.

42. A method for securing data on a computer network including a plurality of users comprising the steps of:

storing security device transaction data in a memory
for ensuring authenticity and authority of one of the plurality
of users, wherein the security device transaction data is related
30 to the one of the plurality of users; and

43. The method of claim 42 further comprising the step of
35 printing the value bearing item.

1 44. The method of claim 42 further comprising the step of
storing a plurality of security device transaction data in a
database wherein, each transaction data is related to one of the
plurality of users.

5 45. The method of claim 44 further comprising the step of
loading a security device transaction data related to the
cryptographic device when the user requests to operate on a value
bearing item.

10 46. The method of claim 42 further comprising the steps of
authenticating the identity of each user and verifying that the
identified user is authorized to assume a role and to perform a
corresponding operation.

15 47. The method of claim 42, wherein the step of determining
a state comprises of determining an uninitialized state.

20 48. The method of claim 42, wherein the step of determining
a state comprises of determining an initialized state.

 49. The method of claim 42, wherein the step of determining
a state comprises of determining an operational state.

25 50. The method of claim 42, wherein the step of determining
a state comprises of determining an administrative state.

 51. The method of claim 42, wherein the step of determining
a state comprises of determining an exporting shares state.

30 52. The method of claim 42, wherein the step of determining
a state comprises of determining an importing shares state.

35 53. The method of claim 42, wherein the step of determining
a state comprises of determining an error state.

1 54. The method of claim 47, wherein the one or more
commands corresponding to the uninitialized state includes a
command for start initializing.

5 55. The method of claim 48, wherein the one or more
commands corresponding to the initialized state includes commands
for one or more of get status command, initialize access control
database command, logon command, logoff command, query current
10 user role command, query current user ID command, session
management commands, audit entry creation command, generate
master key set command, and generate transport key pair commands.

15 56. The method of claim 49, wherein the one or more
commands corresponding to the operational state include commands
for one or more of access control, session management, key
management, and audit support.

20 57. The method of claim 56, wherein the commands for access
control include one or more of transition to administrative state
command, logon command, logoff command, query current user role
command, query current user ID command, view access control
database command, change password command, set clock command, and
set Status command.

25 58. The method of claim 56, wherein the commands for
session management include one or more of open session command,
close Session command, compute session MAC command, verify
session MAC command, session encrypt command, and session decrypt
command.

30 59. The method of claim 56, wherein the commands for key
management include one or more of export transport public key
command, start importing MKS command, create MKS shares command,
generate MKS command, activate MKS command, delete dormant MKS

35

1 command, global decrypt and MAC command, compute MAC command,
verify MAC, and encryption and MAC translation commands.

5 60. The method of claim 56, wherein the commands for audit
support include one or more of create audit entry command, create
audit key command, and export audit verification key command.

10 61. The method of claim 50, wherein the one or more
commands corresponding to the administrative state include
commands for one or more of create account command, delete
account command, modify account command, view access control
database command, end admin. command, logon command, logoff
command, query current user role command, query current user ID
command, set clock command, get status command, session
15 management commands, and audit entry creation command.

20 62. The method of claim 51, wherein the one or more
commands corresponding to the exporting shares state include
commands for one or more of logon command, logoff command, query
Current User Role command, query current user ID command, export
share command, abort export command, get status command, session
management commands, and audit entry creation command.

25 63. The method of claim 52, wherein the one or more
commands corresponding to the importing shares state include
commands for one or more of logon command, logoff command, query
current user role command, query current user ID command, export
transport public key command, import share command, combine
shares command, set status command, session management commands,
30 and audit entry creation command.

35 64. The method of claim 53, wherein the one or more
commands corresponding to the error state include commands for
one or more of get status command, and access control queries
command.

1 65. The method of claim 42, further comprising the step of
printing a postage value including a postal indicium.

5 66. The method of claim 65, wherein the postal indicium
includes a digital signature.

 67. The method of claim 65, wherein the postal indicium
includes a postage amount.

10 68. The method of claim 65, wherein the postal indicium
comprises an ascending register of used postage and descending
register of available postage.

15 69. The method of claim 42, further comprising the step of
printing a ticket.

 70. The method of claim 42, further comprising the step of
printing a bar code.

20 71. The method of claim 42, further comprising the step of
printing a coupon.

 72. A security system for securing data in a computer
network comprising:

25 a plurality of user terminals coupled to the computer
network;

 a cryptographic device remote from the plurality of
user terminals and coupled to the computer network, wherein the
cryptographic device includes a state machine for determining a
30 state corresponding to one or more commands available to an
authenticated user; and

 a plurality of security device transaction data for
ensuring authenticity of the one or more users, wherein each
security device transaction data is related to a user.

35

1 73. The system of claim 72, wherein the security device
transaction data related to a user is loaded into the
cryptographic device when the user requests to operate on a value
bearing item.

5 74. The system of claim 72, wherein the state machine
includes an uninitialized state.

10 75. The system of claim 72, wherein the state machine
includes an initialized state.

 76. The system of claim 72, wherein the state machine
includes an operational state.

15 77. The system of claim 72, wherein the state machine
includes an administrative state.

 78. The system of claim 72, wherein the state machine
includes an exporting shares state.

20 79. The system of claim 72, wherein the state machine
includes an importing shares state.

25 80. The system of claim 72, wherein the state machine
includes an error state.

 81. The system of claim 74, wherein the one or more
commands corresponding to the uninitialized state includes a
command for start initializing.

30 82. The system of claim 75, wherein the one or more
commands corresponding to the initialized state includes commands
for one or more of get status command, initialize access control
database command, logon command, logoff command, query current
35 user role command, query current user ID command, session

83. The system of claim 76, wherein the one or more
5 commands corresponding to the operational state include commands
for one or more of access control, session management, key
management, and audit support.

85. The system of claim 83, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

87. The system of claim 83, wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command.

-90-

1 account command, modify account command, view access control
database command, end admin. command, logon command, logoff
command, query current user role command, query current user ID
command, set clock command, get status command, session
5 management commands, and audit entry creation command.

89. The system of claim 78, wherein the one or more
commands corresponding to the exporting shares state include
commands for one or more of logon command, logoff command, query
10 Current User Role command, query current user ID command, export
share command, abort export command, get status command, session
management commands, and audit entry creation command.

90. The system of claim 79, wherein the one or more
15 commands corresponding to the importing shares state include
commands for one or more of logon command, logoff command, query
current user role command, query current user ID command, export
transport public key command, import share command, combine
shares command, set status command, session management commands,
20 and audit entry creation command.

91. The system of claim 80, wherein the one or more
commands corresponding to the error state include commands for
one or more of get status command, and access control queries
25 command.

92. The system of claim 72 further comprising computer
executable code to keep track of a present operational state.

30 93. The system of claim 72, wherein the processor is
programmed to verify that the authenticated user is authorized
to assume a role and perform a corresponding operation.

94. The system of claim 72, wherein the system includes a
35 computer executable code for supporting multiple concurrent users

1 and maintaining a separation of roles and operations performed
by each user.

5 95. The system of claim 72, wherein the value bearing item
is a postage value including a postal indicium.

96. The system of claim 95, wherein the postal indicium
comprises a digital signature.

10 97. The system of claim 95, wherein the postal indicium
comprises a postage amount.

15 98. The system of claim 95, wherein the postal indicium
comprises an ascending register of used postage and descending
register of available postage.

99. The system of claim 72, wherein the value bearing item
is a ticket.

20 100. The system of claim 72, wherein the value bearing item
includes a bar code.

25 101. The system of claim 72, wherein each security device
transaction data includes information to define the present
operational state of the device.

30 102. The system of claim 72, wherein the cryptographic
engine is programmed to perform one or more of Rivest, Shamir and
Adleman (RSA) public key encryption, DES, Triple-DES, DSA
signature, SHA-1, and Pseudo-random number generation algorithms.

103. The system of claim 72, wherein at least one of the
users is an enterprise account.

35

1 104. A method for secure printing of value-bearing items
over a computer network having a plurality of user terminals, the
method comprising the steps of:

5 storing information about a plurality of users using
the plurality of terminals in a database remote from the
plurality of user terminals;

 securing the information about the users in the
database by one or more of cryptographic devices remote from the
plurality of user terminals;

10 storing a plurality of security device transaction data
in the database, wherein each transaction data is related to one
of the plurality of users; and

 determining a state in a state machine for availability
of one or more commands.

15 105. The method of claim 104 further comprising the step of
printing the value bearing item.

20 106. The method of claim 104 further comprising the step of
loading a security device transaction data related to a user into
one of the one or more of cryptographic devices when the user
requests to operate on a value bearing item.

25 107. The method of claim 104 further comprising the step of
loading a security device transaction data related to the
cryptographic device when the user requests to operate on a value
bearing item.

30 108. The method of claim 104 further comprising the steps
of authenticating the identity of each user and verifying that
the identified user is authorized to assume a role and to perform
a corresponding operation.

35

2025 RELEASE UNDER E.O. 14176

1 109. The method of claim 104, wherein the step of
determining a state comprises of determining an uninitialized state.

5 110. The method of claim 104, wherein the step of
determining a state comprises of determining an initialized
state.

10 111. The method of claim 104, wherein the step of
determining a state comprises of determining an operational
state.

15 112. The method of claim 104, wherein the step of
determining a state comprises of determining an administrative
state.

20 113. The method of claim 104, wherein the step of
determining a state comprises of determining an exporting shares
state.

25 114. The method of claim 104, wherein the step of
determining a state comprises of determining an importing shares
state.

30 115. The method of claim 104, wherein the step of
determining a state comprises of determining an error state.

35 116. The method of claim 104, further comprising the step
of printing a postage value including a postal indicium.

 117. The method of claim 116, wherein the postal indicium
includes a digital signature.

 118. The method of claim 116, wherein the postal indicium
includes a digital signature.

method of claim
age amount.
method of claim
ticket.

[illegible]

35